

PAT-NO: JP411355858A

DOCUMENT-IDENTIFIER: JP 11355858 A

TITLE: INFORMATION DISTRIBUTION METHOD IN
MOBILE COMMUNICATION NETWORK

PUBN-DATE: December 24, 1999

INVENTOR-INFORMATION:

NAME	COUNTRY
SAITO, YUKICHI	N/A
KAMISAKA, KYUICHI	N/A
NAKAMURA, HIROSHI	N/A
TAMURA, MOTOI	N/A
AKIYAMA, DAISUKE	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
NTT MOBIL COMMUN NETWORK INC	N/A

APPL-NO: JP10163939

APPL-DATE: June 11, 1998

INT-CL (IPC): H04Q007/38, H04L009/08 , H04L009/32

ABSTRACT:

PROBLEM TO BE SOLVED: To encrypt distributed information and to distribute the encrypted information with an encryption method with high security, where management of an encryption key is easy.

SOLUTION: An information server 5 encrypts distributed information by an encryption key and encrypts the encryption key, by using an authentication key different by every mobile station. The encrypted encryption

key and the distributed information are transferred to a mobile station 1 at the same time or at different times. The mobile station 1 uses the authentication key possessed by itself to interpret the encrypted encryption key and uses the interpreted encryption key to decode the distributed information.

COPYRIGHT: (C)1999,JPO

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-355858

(43) 公開日 平成11年(1999)12月24日

(51) Int.Cl.⁹

識別記号

F I

H 0 4 Q 7/38

H 0 4 B 7/26

1 0 9 R

H 0 4 L 9/08

H 0 4 L 9/00

6 0 1 A

9/32

6 7 5 A

審査請求 未請求 請求項の数 5 O L (全 7 頁)

(21) 出願番号 特願平10-163939

(22) 出願日 平成10年(1998)6月11日

(71) 出願人 392026693

エヌ・ティ・ティ移動通信網株式会社
東京都港区虎ノ門二丁目10番1号

(72) 発明者 斉藤 祐吉

東京都港区虎ノ門二丁目10番1号 エヌ・
ティ・ティ移動通信網株式会社内

(72) 発明者 上坂 久一

東京都港区虎ノ門二丁目10番1号 エヌ・
ティ・ティ移動通信網株式会社内

(72) 発明者 中村 寛

東京都港区虎ノ門二丁目10番1号 エヌ・
ティ・ティ移動通信網株式会社内

(74) 代理人 弁理士 谷 義一 (外3名)

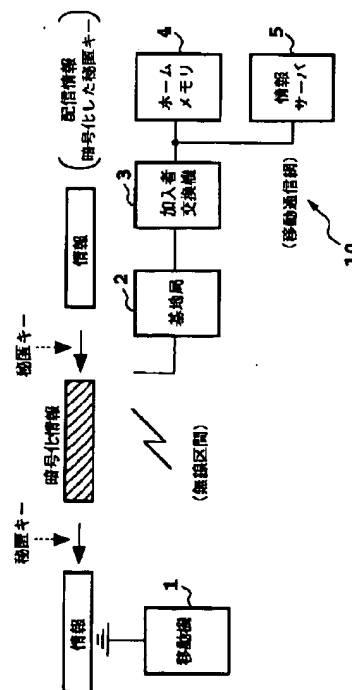
最終頁に続く

(54) 【発明の名称】 移動通信網における情報配信方法

(57) 【要約】

【課題】 秘匿キーの管理が容易で、セキュリティの高い暗号化方法で配信情報を暗号化して配信する。

【解決手段】 情報サーバでは配信情報を秘匿キーにより暗号化すると共に、秘匿キーを移動機毎に異なる認証キーを使用して暗号化する。暗号化された秘匿キーと配信情報とは同時点あるいは異なる時点で移動機1に転送される。移動機1では自己が保有する認証キーを使用して暗号化された秘匿キーを解読し、次に、解読された秘匿キーを使用して配信情報を解読する。



【特許請求の範囲】

【請求項1】 移動通信網内に設置された情報サーバ内に保存された配信情報を暗号化して移動機に配信する移動通信網における情報配信方法において、前記情報サーバ側では秘匿キーを使用して前記配信情報を暗号化し、配信対象の移動機の認証に使用する認証キーを使用して前記秘匿キーを暗号化し、当該暗号化された秘匿キーおよび配信情報を前記配信対象の移動機に送信し、前記配信対象の移動機では、暗号化されて送信された秘匿キーを自己が保有する認証キーを使用して解読し、当該解読された秘匿キーを使用して暗号化されて送信された配信情報を解読することを特徴とする移動通信網における情報配信方法。

【請求項2】 請求項1に記載の移動通信網における情報配信方法において、暗号化された前記秘匿キーと暗号化された配信情報を異なる時点で前記情報サーバから前記配信対象の移動機に対して転送することを特徴とする移動通信網における情報配信方法。

【請求項3】 請求項1に記載の移動通信網における情報配信方法において、暗号化された前記秘匿キーと暗号化された配信情報を同時点で前記情報サーバから前記配信対象の移動機に対して転送することを特徴とする移動通信網における情報配信方法。

【請求項4】 請求項1に記載の移動通信網における情報配信方法において、前記秘匿キーを所定タイミングで変更することを特徴とする移動通信網における情報配信方法。

【請求項5】 請求項1に記載の移動通信網における情報配信方法において、前記認証キーおよび前記秘匿キーを記憶するホームメモリを前記移動通信網内に設置し、該ホームメモリから前記情報サーバに対して前記認証キーおよび前記秘匿キーを引き渡すことを特徴とする移動通信網における情報配信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、移動通信網において情報の配信のために情報を暗号化する場合の秘匿キーを移動機に設定するための移動通信網における情報配信方法に関する。

【0002】

【従来の技術】移動通信網においても情報配信サービスが行われている。移動通信網内には情報サーバが設置されており、所定時刻になると、情報サーバ内に記憶されていた配信情報が所定の移動機に対して配信される。このような配信情報は、特定の移動機に対してのみ配信されるためにユーザから情報の秘匿性を求められることが多くなっている。通信の分野では、通信情報を秘匿するためには暗号化を行っている。暗号化の一般的な方

法は情報の送信元は秘匿キー（ある特定の数値等、秘匿キーとも呼ばれる）と暗号化のための演算式とを使用して、情報たとえば、文字コード列を他の文字コード列に変換する。暗号化された情報（文字コード列）を受信した送信先では上記秘匿キーと同じ秘匿キーと暗号化とは逆の演算式を使用して、暗号化された情報を解読（復号化とも呼ばれる）する。

【0003】このような暗号化方法を使用する場合に移動通信では次の点が重要となる。

10 【0004】1. 情報内容が無線で伝送されるので、盗聴の危険性が大きく、秘匿キーを誰にも知られないようにしておきたい。

【0005】2. 配信情報サービスを受ける移動機は多数なので、移動機毎に秘匿キーを異ならせたい。

【0006】

【発明が解決しようとする課題】上記第1の点を満足するためには2つの方法が知られている。第1の方法では、秘匿キーをROMなどに記憶し、人間の指示では上記秘匿キーを読み出せないように秘匿キーをROMに閉じ込める。この方法は、ROMを外してROMリードにかけるとROMの記憶内容が読み出されてしまうという欠点と、一度秘匿キーを定めるとその秘匿キーを変更することは困難という欠点がある。

【0007】第2の方法は、情報送信元が秘匿キーを一定時間毎に変更し、暗号化したときに使用した秘匿キーを暗号文と共に送信元から送信先へ送信する。送信先では受信された秘匿キーで暗号文を解読する。この方法は秘匿キーそのものが盗聴の危険性がある。

30 【0008】上記第2の点を満足させるためには、情報の送信元では移動機毎、たとえば、加入者番号毎に秘匿キーを記憶しなければならないので、その情報管理が大変な労力となる。また、秘匿キーを一定時間間隔で変更させたい場合を考慮すると記憶している秘匿キーの変更処理を行うコンピュータシステムに大きな負担がかかる。

【0009】そこで、本発明は、秘匿キーを使用して配信情報を暗号化して配信する際に、移動通信網側の秘匿キーの管理が容易で、かつ、秘匿キーの変更が可能かつ、秘匿キーおよび配信情報の秘匿性が高い移動通信網における情報配信方法を提供することにある。

【0010】

【課題を解決するための手段】このような目的を達成するために、請求項1の発明は、移動通信網内に設置された情報サーバ内に保存された配信情報を暗号化して移動機に配信する移動通信網における情報配信方法において、前記情報サーバ側では秘匿キーを使用して前記配信情報を暗号化し、配信対象の移動機の認証に使用する認証キーを使用して前記秘匿キーを暗号化し、当該暗号化された秘匿キーおよび配信情報を前記配信対象の移動機に送信し、前記配信対象の移動機では、暗号化されて送

信された秘匿キーを自己が保有する認証キーを使用して
 解読し、当該解読された秘匿キーを使用して暗号化され
 て送信された配信情報を解読することを特徴とする。

【0011】請求項2の発明は、請求項1に記載の移動
 通信網における情報配信方法において、暗号化された前
 記秘匿キーと暗号化された配信情報を異なる時点で前記
 情報サーバから前記配信対象の移動機に対して転送する
 ことを特徴とする。

【0012】請求項3の発明は、請求項1に記載の移動
 通信網における情報配信方法において、暗号化された前
 記秘匿キーと暗号化された配信情報を同時点で前記情報
 サーバから前記配信対象の移動機に対して転送すること
 を特徴とする。

【0013】請求項4の発明は、請求項1に記載の移動
 通信網における情報配信方法において、前記秘匿キーを
 所定タイミングで変更することを特徴とする。

【0014】請求項5の発明の発明は、請求項1に記載
 の移動通信網における情報配信方法において、前記認証
 キーおよび前記秘匿キーを記憶するホームメモリを前記
 移動通信網内に設置し、該ホームメモリから前記情報サ
 ーバに対して前記認証キーおよび前記秘匿キーを引き渡
 すことを特徴とする。

【0015】

【発明の実施の形態】図面を参照して、本発明の実施形
 態を詳細に説明する。

【0016】図1に移動通信網におけるシステム構成と
 情報の流れを示す。図1において、1は移動機であり、
 配信情報を受信し、移動機1の表示器に配信情報を表示
 する。移動機1の回路構成は従来と同様のものを使用す
 ることができるが、配信情報の解読に係る秘匿キーが暗
 号化され、その暗号化されている秘匿キーを解読するた
 めの処理手順を実行する点が従来と異なる。このような
 処理手順はたとえば、移動機1内のROMなどに記憶さ
 れ、移動機1内のCPUあるいはデジタルプロセッサに
 より実行される。

【0017】2は基地局であり、移動機1との間で無線
 により情報の授受を行う。3は加入者交換機であり、加
 入者交換機3は基地局2、移動通信網10内で他の交換
 機、ホームメモリ4、情報サーバ5との間で情報の授受
 を行う。

【0018】基地局3および加入者交換機4は従来と同
 様とすることができるので、詳細な説明を要しないであ
 ろう。4はホームメモリであり、ホームメモリ4は移動
 通信網10内に設置され、移動機1の加入者番号（いわ
 ゆる電話番号）および通信パケットアドレス、認証キー
 および秘匿キー、その他、加入者に関する各種の情報を
 記憶し、管理する。認証キー自体は周知であるが本発明
 に係るので、簡単に説明しておく。認証キーは、移動機
 1の認証に使用するコードであり、通信契約がユーザ
 （加入者）と移動通信サービス会社との間に結ばれた際

に、認証キーが決定される。認証キーは移動機毎に異な
 り、セキュリティのために、最初の通信時に無線区間を
 送信するのではなく、オペレータの視点等で直接不揮発
 性メモリ内に書き込まれ保存される。

【0019】移動通信網10側で認証時（位置登録、通
 信開始に先だって行われる手順）に乱数を発生させ、そ
 の乱数を移動機1に転送する。

【0020】ネットワークはホームメモリに蓄えられて
 いる、あるユーザの認証キーを基に、乱数と秘匿キーを
 使って演算を行う。

【0021】移動機1も転送されてきた乱数を基に自身
 が持っている秘匿キーを使って演算を行い、その演算結
 果を移動通信網10へ返送する。

【0022】移動通信網10では、自身の演算結果と移
 動機が返送してきた演算結果を照合し、一致していれば
 認証オーケーで位置登録、通信開始手順を継続する。

【0023】双方が一致したときに移動機1が移動通信
 サービス会社と契約したものであると認証される。

【0024】この認証に使用される認証キーがホームメ
 モリ4に保存されている点に本願発明者は着目し、上述
 の秘匿キーを上記認証キーを使用して第1の暗号化、転
 送を行い、秘匿キーを使用して配信情報を第2の暗号
 化、転送する点が本実施形態の大きな特徴である。この
 ため、秘匿キーはユーザ毎に異なる認証キーにより暗号
 化されるので、秘匿キーが単一でも暗号化された秘匿キ
 ーはユーザ毎に異なったものとなる。したがって、ホー
 ムメモリ4は単一の秘匿キーを管理すればよい。本実施
 形態では、さらにホームメモリ4は一定時間間隔で上記
 秘匿キーをランダム（乱数的）に変更するがこの変更処
 理をも簡単に行うことができる。さらに秘匿キーと配信
 情報は異なるキーで暗号化されるので、単一の暗号化ア
 ルゴリズムを使用しても秘匿キーおよび配信情報の秘匿
 性が高いものとなる。なお、本実施形態では、秘匿キー
 の暗号化アルゴリズム（演算式）と配信情報の暗号化ア
 ルゴリズムは異ならせている。

【0025】図1に戻り、5は情報サーバであり、配信
 すべき情報、配信先の移動機に関する加入者番号、移動
 通信のための通信パケットアドレス等の情報を記憶す
 る。

【0026】複数の基地局1、複数の加入者交換機1、
 複数のホームメモリ4、1以上の情報サーバ5は有線の
 信号線で接続され、移動通信に関する制御情報や通話情
 報、配信情報を関連者間で転送する。

【0027】このようなシステム構成において行われる
 配信情報の配信処理を図2～図5を参照して説明する。
 図2は配信処理にかかわる通信基本シーケンスの内容を示
 す。

【0028】図3は情報サーバ5の配信に係る処理手順
 を示す。図4はホームメモリ4の配信に係る処理手順を
 示す。図4は配信情報を受け取る移動機1の処理手順を

示す。

【0029】情報サーバ5では内部に記憶されている配信スケジュールに従って、現在の時刻に配信すべき配信情報があるか否かを判定する(図3のステップS100)。現在の時刻に配信すべき配信情報がある場合に情報サーバ5は登録されている移動機1に対して、呼び出しを行う。この呼び出しは、通常の通話と同様、加入者番号による呼び出しを行う形態をとってもよいし、配信情報を配信する旨の識別子をもたせた呼びかけを意味する通信パケットを加入者交換機3、基地局1を介して移動機1に送信する形態をとってもよい。この呼び出しを移動機1が受信すると(図5のステップS300)、移動機1では呼び出しに回答し、次に認証要求を待つ(図5のステップS310→S320)。

【0030】移動機1からの回答を基地局2、加入者交換機3を介して受けたホームメモリ4では、移動機1に対応する登録の認証キーを加入者交換機3に送信する。加入者交換機3は従来と同様にして移動機1に対して認証要求を基地局2経由で送信する(図4のステップS200→S210)。

【0031】認証要求を受けた移動機1では内部に記憶してある秘匿キーを使用して演算を行いその演算結果を基地局2に送信する(図5のステップS320→S330)。本実施形態では加入者交換機3において移動通信網側での演算結果と移動機1側からの演算結果との照合を行う。この照合において、一致の判定、すなわち、認証成功の判定が行われると、移動機1と基地局2との間の無線区間の設定、加入者交換機3、ホームメモリ4、情報サーバ5間の中継区間の設定が行われ、移動機1と情報サーバ5との接続が行われる。以上までの処理手順は従来と同様である。

【0032】認証キーによる認証後、情報サーバ5はホームメモリ4に対して秘匿キーおよび認証キーの送信要求をホームメモリ4に対して送信し、ホームメモリ4から認証キーおよび秘匿キーを受信する(図3のステップS120)。情報サーバ5は受信した認証キーを使用して秘匿キーを暗号化する(図3のステップS130)。暗号化のアルゴリズム自体は本発明を実施する上でのセキュリティの問題から開示できないので、仮の暗号化方法を説明する。一例としては、認証キーの示す数値(たとえば、10進数で5)と秘匿キーの示す数値(たとえば、10進法で3)を乗算する。その乗算結果(数値15)が暗号化された秘匿キーの値となる。異なる移動機1に対してはその認証キーが数値4とすると暗号化された秘匿キーの値は $4 \times 3 = 12$ となり、上述の値15と互いに異なることに注意されたい。当然のことながら秘匿キーの値3とも異なることは言うまでもない。

【0033】次に情報サーバ5は秘匿キーを使用して秘匿キーの暗号化方法とは異なる第2の暗号化方法で秘匿キーを暗号化する。送信する配信情報が文字コード列と

すると、文字コード列の各文字コードの示す数値に秘匿キーの値(この場合3)を加算して暗号化した文字コード列を作成する(図3のステップS140)。

【0034】このようにして第1の暗号化方法により暗号化された秘匿キーおよび第2の暗号化方法により暗号化された配信情報は配信指定された移動機(配信対象の移動機)1に対して配信される(図3のステップS150)。

【0035】認証手順終了後、暗号化された秘匿キーおよび配信情報を受信し(図5のステップS340)、秘匿キーを最初に解読する(図5のステップS350)。暗号化された秘匿キーの値は15(5×3)であるので、自己が保存する照合用の認証キー(数値5)を使用して乗算の逆すなわち、暗号化された値15を照合用の認証キーの値5で除算して秘匿キーの値を取得する。

【0036】次に移動機1では秘匿キーの値を使用して、受信した配信情報の解読を行う。この例では秘匿キーの加算により暗号化が行われるので、暗号化された文字コード列の各文字コードの値から秘匿キーの値3を減算して配信情報の復号化を行う(図5のステップS360)。解読(復号化)された配信情報は移動機1の表示器に表示される(図5のステップS370)。

【0037】ホームメモリ4では情報サーバ5の要求に応じて認証キーおよび秘匿キーを送信した後(図4のステップS230の後)、図4のステップS200→S240→S260の手順を繰り返して、秘匿キーの変更時刻になるのを待つ。たとえば、前回の秘匿キーの変更から1時間が経過し、変更時刻に到達したことをホームメモリ1が検知すると(図4のステップS240のYES判定)、ホームメモリ4はたとえば、乱数器を使用して新規の秘匿キーを発生する。作成された秘匿キーは内部の記憶装置に保存され、次の変更があるまでの間、情報サーバ5側の暗号化のために使用される。以下、一定時刻を経過するごとに秘匿キーは変更される。

【0038】以上の配信処理では、移動機1側では、暗号化され、時刻によって異なる秘匿キーを受信するので、暗号解読のための演算式(アルゴリズム)は他の移動機1と同じものを使用することができる。また、基地局2と複数の移動機1との間で無線で配信情報が伝送されても、伝送される暗号化された秘匿キーの値は移動機毎に異なるので、たとえ、無線を盗聴しても、その盗聴情報に秘匿キーが含まれることすら識別できないであろう。

【0039】さらにホームメモリ4では単一の秘匿コードを所定時間毎に(間隔は一定にする必要はない)変更すればよいので、秘匿コードの管理(保存、変更)が非常に容易である。

【0040】上述の実施形態の他に次の形態を実施できる。

【0041】1) 上述の実施形態では、秘匿キーを変更

している。暗号化された秘匿キーと配信情報を異なる暗号方法で暗号化し移動機1に配信しているが、秘匿キーを固定化したい場合には、秘匿キーと配信情報を異なるタイミングで情報サーバから配信するとよい。この場合には、暗号化方法を共通化できる。暗号化された秘匿キーの送信タイミングとしては、移動機1から位置登録要求があった時点や、発信があった時点とすることができる。

【0042】2) 上述の実施形態では、秘匿キーをホームメモリ4が管理し、配信情報を情報サーバ5が管理しているが、秘匿キーを情報サーバ5に管理させてもよい。

【0043】3) 秘匿キーおよび配信情報を暗号化するための暗号化方法は任意の方法を使用することができる。

【0044】4) 上述の実施形態では、移動機1の表示器に配信情報を表示させる形態を説明したが、移動機1に接続された端末、たとえば、電子手帳等やモバイルコンピュータと呼ばれる情報処理装置により配信情報を表示してもよい。

【0045】5) 上述の実施形態では単一種の秘匿コードを使用する形態を説明したが、この秘匿コードは同報通信の様に、配信情報を複数の同報通信者に通信する場合に使用するとよい。情報配信サービス契約者が異なる場合には秘匿コードを異ならせればよいことは言うまでもないであろう。

【0046】6) 配信情報は文字に限らず、イメージ、音声、HTML言語で記載された文書情報、あるいはこれら情報が混在した情報、端末側で実行するソフトウェアプログラム（アプリケーションプログラムとも呼ばれる）等、各種の情報を取り扱うことができる。

【0047】

【発明の効果】以上、説明したように、請求項1の発明では、配信情報の暗号化に使用した秘匿キーをも暗号化して移動機側に転送するので、移動機側では秘匿キーを保持する必要がなく、秘匿キーを配信情報の送信側で自由に変えることができる。さらに秘匿キーを認証キーを使用して暗号化することにより暗号化された秘匿キーの内容は移動機毎に異なるので、たとえ、暗号化された秘

匿キーが盗聴されても、秘匿キーそのものの安全性が図られる。さらには秘匿キー自体は認証番号毎、すなわち、移動機毎に設定する必要はないので、秘匿キーの種類を少なくでき、秘匿キーの管理が容易となる。

【0048】請求項2の発明では、暗号化された秘匿キーと配信情報の送信タイミングを異ならせることにより、共通の暗号化方法で暗号化を行っても、その秘匿性が損なわれることはない。

【0049】請求項3の発明では、暗号化された秘匿キーと配信情報を同時点で送信することにより秘匿キーを変更しても受信側の移動機では受信の秘匿キーを使用すればよく、配信情報の送信タイミングあるいは秘匿情報の更新タイミングに制約を与えることはない。

【0050】請求項4の発明では、秘匿キーを変更することにより、秘匿キー、ひいては配信情報の安全性、秘匿性が高まる。

【0051】請求項5の発明では、認証キーおよび秘匿キー等の秘匿性に係る情報を配信情報を記憶しておく情報サーバとは別のホームメモリに記憶しておくことで、配信情報および上記認証キーおよび秘匿キーの暗号解読に係るキーの全部を入手することは困難となる。

【図面の簡単な説明】

【図1】本発明実施形態の配信処理手順を示す説明図である。

【図2】本発明実施形態のシステム構成および情報の流れを示す構成図である。

【図3】図1の情報サーバ5の処理手順を示すフローチャートである。

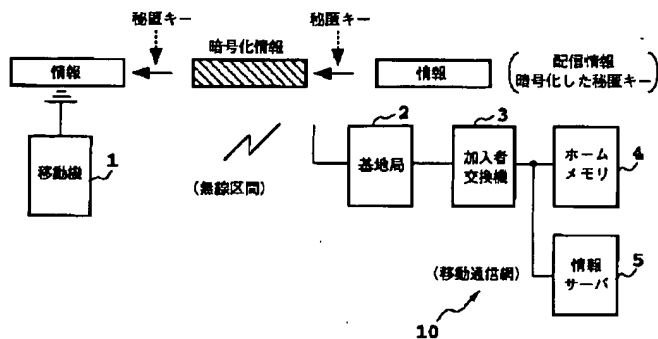
【図4】図1のホームメモリの処理手順を示すフローチャートである。

【図5】図1の移動機の処理手順を示すフローチャートである。

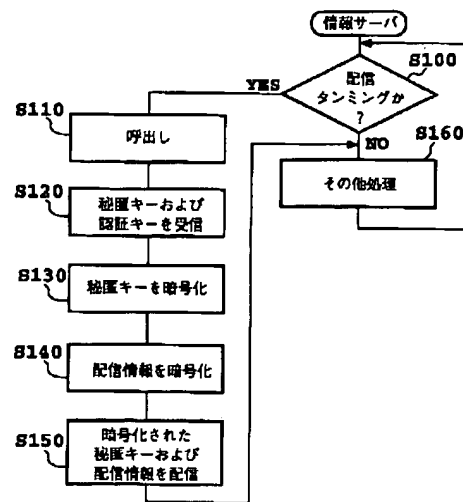
【符号の説明】

- 1 移動機
- 2 基地局
- 3 加入者交換機
- 4 ホームメモリ
- 5 情報サーバ

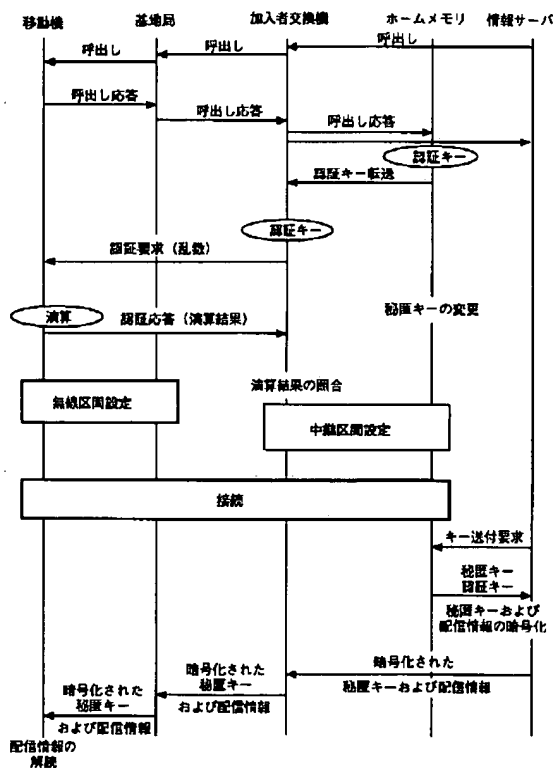
【図 1】



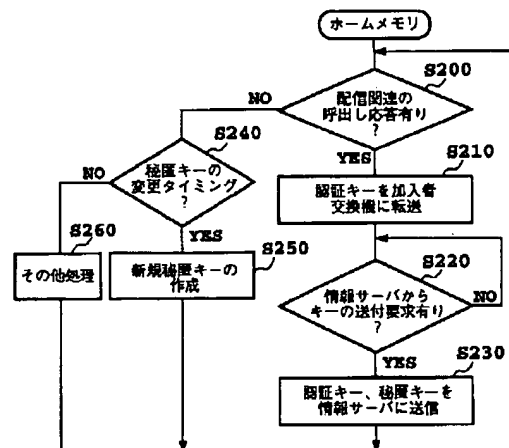
【図3】



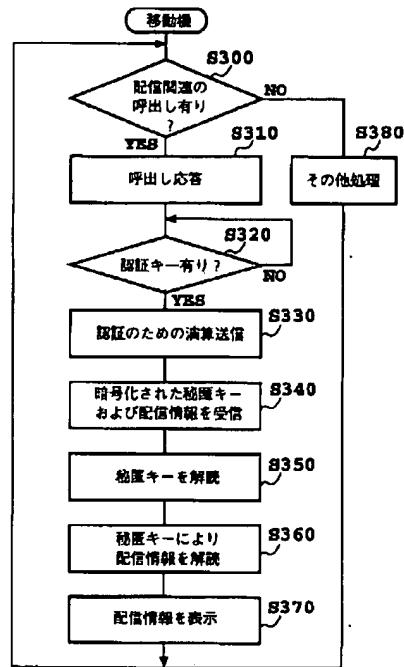
【図2】



【図4】



【図5】



フロントページの続き

(72)発明者 田村 基
東京都港区虎ノ門二丁目10番1号 エヌ・
ティ・ティ移動通信網株式会社内

(72)発明者 秋山 大介
東京都港区虎ノ門二丁目10番1号 エヌ・
ティ・ティ移動通信網株式会社内